REMARKS

Claims 1-187 and 189-193 are currently pending. Applicants respectfully request reconsideration of the above-identified application in light of the following remarks.

Claim Rejections Under 35 U.S.C. §102

1. Claims 1-15, 19-27, 55-61, 73-81, 100-112, 121, 122, 126, 128, 129, 130, 140-149, 155-159, 162-164, 172-174, 177-179, 180-182, 189, and 190-193 have been rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5, 371,797 to Bocinsky ("Bocinsky"). Applicants respectfully traverse this rejection.

Bocinsky cannot anticipate these claims because it does not teach or suggest each and every element of these claims. See MPEP §2131 (*quoting* Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631 (Fed. Cir. 1987) ("[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference")).

Independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189 recite a "sender-defined security attribute" (emphasis added). Independent claims 1, 28, 55, 82, 109, 111, 115, 117 and 189 recite, "wherein the at least one sender-defined security attribute is defined at the time of an electronic fund transfer" (emphasis added); independent claims 19, 73 and 110, recite, "wherein the at least one sender-defined security attribute is defined at the time a sender sends the digital rights management container" (emphasis added); and claims 46, 100, 113, 116 and 119 recite, "wherein the at least one sender-defined security attribute is defined at the time a sender sends the secure file" (emphasis added).

In contrast, Bocinsky describes a system and apparatus in which an encrypted PIN is defined by a computer prior to the time of a transaction, during a separate, preceding event. Additionally, this encrypted PIN is created through the use of a secure network.

Bocinsky describes a system and method involving at least two main stages. In the first stage, a "secure transaction processor" (Bocinsky, Abstract, line 8), such as a secure point of sale terminal (Bocinsky, col. 4, line 24), is utilized to encrypt a PIN. The PIN is encrypted using a key that is "acquired from either a specific request to, or monitoring data passing from a conventional network security transaction processor" (Bocinsky, Abstract, lines 12-15). This encrypted PIN is broken into two parts, one is provided to the user, the other is stored in the system. Figure 3 of Bocinsky illustrates the parsing of the encryption key (62) into two segments, storing of an N-M character length segment (65), and transmission of an M-character length segment to the customer (68). This first stage allows for the second stage to occur securely. More specifically, the M-character length segment is later used in the second stage by the customer when using an insecure network to perform a transaction.

In the second stage, an insecure network (such as a telephone system), is used to perform a financial transaction using a portion of the encrypted PIN (M-character length segment) generated during the first stage. This process is illustrated in Figure 4 of Bocinsky. The only action required on the part of the customer, at the time of performing a transaction, is inputting pre-determined values into the system ("TSAN" in 75, "M-char" in 77). The system then "concatenates" the provided M-character length segment to the N-M-character length segment to reconstitute the N-character length segment. Nothing during the transaction is being "defined," as required by independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189. Rather, these values have all been pre-determined in one way or another. If

anything in Bocinsky, is "defined," the definition occurs in the first stage, *not* during this second stage during which the actual transaction is occurring.

The Office Action argues:

> ...the process of providing the access code, which is unmasked with second portion to recreate the original full encrypted PIN is readable [as] a security attribute that is defined at the time of the fund transfer...

and that

> ...the security attribute is interpreted as the customer security identification such as PIN number that also includes encryption key, password and so....

See Office Action at page 3.

Applicants appreciate the insight provided by the Examiner as to how he is interpreting the Bocinsky patent. However, Applicants respectfully submit that the alleged "definition" does not occur at the time of a fund transfer, and that the recreation of the original full encrypted PIN does not constitute a "definition." In contrast, it is indeed, only a "recreation." The encrypted PIN had been previously "defined" in the above-described first stage, and during the transaction is merely being "reconstituted" (or recreated).

While the customer in Bocinsky is "providing" an access code, the customer is not "defining" the access code at the time of the transaction, as required by independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189. Merriam-Webster on-line dictionary (www.m-w.com) defines the verb to "provide," in the most fitting sense, as "to supply or make available." In contrast, Merriam-Webster on-line dictionary defines the verb to "define," as to "determine or identify the essential qualities or meaning of," to "fix or mark the

limits of," to "characterize" or to "distinguish." There is a clear difference between these terms, and they are not interchangeable.

Even if the access code (Bocinsky, Abstract, line 19) were considered to be "defined by the user," which Applicants maintain it is not, such definition would occur in a first stage, prior to any actual financial transaction. Bocinsky states that the action occurring during the transaction is "concatenation" ("linking together in a series or chain," see Merriam-Webster on-line dictionary).

The access code is simply being re-united with the other portion of the encrypted PIN. No "definition" occurs at this stage, only what may be considered a reconstitution of a *previously* "defined," encrypted PIN.

Additionally, while the claimed invention, as defined by claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189, may be carried out completely over insecure networks (such as the internet), Bocinsky requires the use of a secure network for the creation of an encrypted PIN. Thus, even if Bocinsky taught or suggested every other feature of the claimed invention (which it does not), the benefits of the present invention, as claimed, could not be fully realized through the practice of Bocinsky. Traditional networks such as that contemplated by Bocinsky allow for anyone with an encryption key to use the data and take it anywhere he or she wishes, while the claimed invention protects the data even in an insecure network.

The invention as claimed, provides security through an object itself (e.g. the "digital rights management container"), and not through the use of a network, as described by Bocinsky. In Bocinsky, the network is used in and relied on in both in creating the encrypted PIN and in using the encrypted PIN to perform a transaction. In the present invention, as claimed, while a "network" such as the internet may be used for transmission in the present

invention, permission to access the object is not provided by the network, but by the object (e.g. the "digital rights management container"), itself. A comparison of the prior art and the claimed invention is analogous to "securing just a pipe" for the prior art, and "securing the pipe and the ends of a pipe," for the invention as claimed. Since one "pipe" for the claimed invention may be the internet, complete security cannot be assured by Bocinsky, but can be by the claimed invention.

For at least the foregoing reasons, independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189, and claims depending from these claims, define patentable subject matter over Bocinsky. Withdrawal of the rejection applied to claims 1-15, 19-27, 55-61, 73-81, 100-112, 121, 122, 126, 128, 129, 130, 140-149, 155-159, 162-164, 172-174, 177-179, 180-182, 189, and 190-193 under 35 U.S.C. §102(b) as being anticipated by Bocinsky is respectfully requested.

Claim Rejections Under 35 U.S.C. §103

2. Claims 16-18, 28-54, 62-72, 82-99, 113-120, 123, 124, 125, 127, 131-139, 150-154, 160, 161, 165-169, 170, 171, 175, 176 and 183 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Bocinsky. Applicants respectfully traverse this rejection.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." (MPEP § 2143.03 (citing In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974))).

As described above, Bocinsky does not teach or suggest each and every element of independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189, and thus these claims define patentable subject matter over Bocinsky. Each of the rejected claims

depends from one of these independent claims, and therefore also defines patentable subject matter over Bocinsky.

Withdrawal of the rejection applied to claims 16-18, 28-54, 62-72, 82-99, 113-120, 123, 124, 125, 127, 131-139, 150-154, 160, 161, 165-169, 170, 171, 175, 176 and 183, under 35 U.S.C. §103(a), as being unpatentable over Bocinsky, is respectfully requested.

CONCLUSION

In light of the foregoing, Applicants believe that all claims, as currently presented, are patentable, and that this application is in condition for allowance.

In the event that a telephonic or personal interview would facilitate the examination of this application in any way, Applicant and his Attorneys hereby invite the Examiner to contact the undersigned at the number provided.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: October 21, 2003

Michael J. Pollack
Registration No. 53,475
(212) 758-4800 Telephone
(212) 751-6849 Facsimile

Correspondence Address:
MORGAN & FINNEGAN, L.L.P.
345 Park Avenue
New York, NY 10154-0053